WHAT IS CLAIMED IS:

1. A system for detecting an illegal loading of a software with a software serial number and executing the software thereafter, the system comprising:

a personal identity circuit for holding a software serial number of a software and generating an inspection code in installing the software; and

a communication control interface having a communication equipment serial number, the communication control interface is provided for connecting the personal identity circuit with a new product registration center, therefore the new product registration center reset the inspection code according to the software serial number and the communication equipment serial number;

wherein the software automatically checks the inspection code before executing the software, when the inspection code is in a legal user state, executing of the software permitted, when the inspection code is in an illegal user state, executing of the software is terminated immediately.

2. The system of claim 1, wherein the new product registration center further comprises a database having a plurality of datasets, when the software serial number and the communication equipment serial number is received by the new product registration center, the software serial number and the communication equipment serial number are compared with the the datasets, when identical software serial number and communication equipment serial number is not found among the datasets, the software serial number and the communication equipment serial number are written down as a new dataset in the database and then the inspection code is reset to the legal user state.

3. The system of claim 2, wherein the new product registration center is connected to a software manufacturer system for reporting a software registration to the

software manufacturer system after the new product registration center reset the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

4. The system of claim 1, wherein the new product registration center further comprises a database having a plurality of datasets, when the software serial number and the communication equipment serial number is received by the new product registration center, the software serial number and the communication equipment serial number are compared with the datasets, when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code is reset to the illegal user state.

5. The system of claim 1, wherein the communication control interface comprises a network interface card.

6. The system of claim 1, wherein the communication control interface comprises a wireless communication network.

7. The system of claim 1, wherein the communication control interface comprises a global positioning system.

8. The system of claim 1, wherein the new product registration center is connected to a software manufacturer system for reporting a software registration to the software manufacturer system after the new product registration center reset the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

9. The system of claim 1, wherein the personal identity circuit further comprises:

a microprocessor having a memory unit for generating the inspection code when installing the software;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

10. The system of claim 9, wherein the memory unit comprises an erasable programmable read-only-memory.

11. They system of claim 9, wherein the memory unit comprises an electrically erasable programmable read-only-memory.

12. The system of claim 9, wherein the memory unit comprises a flash memory.

13. The system of claim 9, wherein the memory unit comprises a static random access memory.

14. The system of claim 9, wherein the memory unit comprises a dynamic random access memory.

15. The system of claim 9, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

16. The system of claim 9, wherein the non-volatile memory unit comprises an electrically erasable read-only-memory.

17. The system of claim 9, wherein the non-volatile memory comprises a flash memory.

18. The system of claim 1, wherein the personal identity circuit further comprises:

a microprocessor having a memory unit for generating the inspection code when installing the software;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

19. A chip in a system for detecting an illegal loading of a software with a software serial number and executing the software thereafter, the chip comprising:

a microprocessor for generating an inspection code when installing a software having a software serial number;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and a communication control interface for transmitting the inspection code and a communication equipment serial number to a new product registration center via the communication control interface such that the new product registration center resets the inspection code according to the received software serial number and the communication equipment serial number, wherein the software automatically checks the inspection code before executing the software, when the inspection code is in a legal user state, executing of the software is permitted, when the inspection code is in an illegal user state, executing of the software is terminated immediately.

20. The chip of claim 19, wherein the communication control interface comprises a network interface card.

21. The chip of claim 19, wherein the communication control interface comprises a wireless communication network.

22. The chip of claim 19, wherein the communication control interface comprises a global positioning system.

23. The chip of claim 19, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

24. They chip of claim 19, wherein the non-volatile memory unit comprises an electrically erasable programmable read-only-memory.

25. The chip of claim 19, wherein the non-volatile memory unit comprises a flash memory.

26. A method of using hardware to detect an illegal loading of a software with a software serial number and executing the software thereafter, comprising:

writing down a software serial number and generating an inspection code when installing a software into a computer; and

transmitting the inspection code and a communication equipment serial number of the computer to a new product registration center;

wherein the new product registration center resets the inspection code according to the received software serial number and the communication equipment serial number, before the computer is able to execute the software, the software automatically checks the inspection code, when the inspection code is in a legal user state, executing of the software is permitted, when the inspection code is in an illegal user state, executing of the software is terminated immediately.

27. The method of claim 26, wherein the new product registration center further comprises a database having a plurality of datasets, when the software serial number

and the communication equipment serial number is received by the new product registration center, the software serial number and the communication equipment serial number are compared with the datasets, when identical software serial number and communication equipment serial number are not found among the datasets, the software serial number and the communication equipment serial number are written down as a new dataset in the database and then the inspection code is reset to the legal user state.

28. The method of claim 27, wherein the new product registration center is connected to a software manufacturer system for reporting a registration of software to the software manufacturer system after the new product registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

29. The method of claim 26, wherein the new product registration center further comprises a database having a plurality of datasets, when the software serial number and the communication equipment serial number is received by the new product registration center, the software serial number and the communication equipment serial number are compared with the datasets, when the software serial number is found within one of the database but a communication equipment serial number in the one of the dataset differs from the received communication equipment serial number, the inspection code is reset to the illegal user state.

30. The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center through a network interface.

31. The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center through a wireless communication network.

32. The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center through a global positioning system.

33. The method of claim 26, wherein the new product registration center is connected to a software manufacturer system for reporting a registration of software to the software manufacturer system after the new product registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

34. A computer system for detecting an illegal loading of a software with a software serial number into the computer system and executing the software thereafter, the computer system comprising:

a microprocessor for generating an inspection code when installing the software to the computer system;

a non-volatile memory coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and a communication control interface for transmitting the inspection code and a communication equipment serial number to the new product registration center via the communication control interface such that the new product registration center resets the inspection code according to the received software serial number and the communication equipment serial number, wherein the software automatically checks

the inspection code before executing the software, when the inspection code is in a legal user state, executing of the software is permitted, when the inspection code is in an illegal user state, executing the software is terminated immediately.

35. The computer system of claim 34, wherein the communication control interface comprises a network interface card.

36. The computer system of claim 34, wherein the communication control interface comprises a wireless communication network.

37. The computer system of claim 34, wherein the communication control interface comprises a global positioning system.

38. The computer system of claim 34, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

39. They computer system of claim 34, wherein the non-volatile memory unit comprises an electrically erasable programmable read-only-memory.

40. The computer system of claim 34, wherein the memory unit comprises a flash memory.

41. A software registration center linked to a hardware system for detecting an illegal loading of a software with a software serial number into a computer and executing the software thereafter, wherein the software registration center has a database with a plurality of datasets, when the software registration center receives the software serial number and the communication equipment serial number, the software serial number and the communication equipment serial number are compared with the datasets, an inspection code stored in the computer is then reset according to the software serial number and the communication equipment serial number, before the computer is able to execute the software, the software automatically checks the

inspection code, when the inspection code is in a legal user state, executing of the software is permitted, when the inspection code is in an illegal user state, executing of the software is terminated immediately.

42. The software registration center of claim 41, wherein the software serial number and the communication equipment serial number received by the software registration center are compared with the datasets, when identical software serial number and communication equipment serial number are not found among the datasets, the software serial number and the communication equipment serial number are written down as a new dataset in the database and then the inspection code is reset to the legal user state.

43. The software registration center of claim 42, wherein the software registration center is connected to a software manufacturer system for reporting an registration of the software to the software manufacturer system after the software registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

44. The software registration center of claim 41, wherein the software serial number and the communication equipment serial number received by the software registration center are compared with the datasets of the database, when the software serial number is found within one of the database but a communication equipment serial number in the one of the dataset differs from the received communication equipment serial number, the inspection code is reset to the illegal user state.

45. The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the software registration center through a network interface.

46. The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the software registration center through a wireless communication network.

47. The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the software registration center through a global positioning system.

48. The software registration center of claim 41, wherein the software registration center is connected to a software manufacturer system for reporting a registration of the software to the software manufacturer system after the software registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.